COUNTING DECOMPOSABLE MULTIVARIATE POLYNOMIALS

Joachim von zur Gathen

July 1, 2009

Abstract. A polynomial f (multivariate over a field) is *decomposable* if $f = g \circ h$ with g univariate of degree at least 2. We determine the dimension (over an algebraically closed field) of the set of decomposables, and an approximation to their number over a finite field. The relative error in our approximations is exponentially decaying in the input size.

Keywords. computer algebra, polynomial decomposition, multivariate polynomials, finite fields, combinatorics on polynomials

1. Introduction

It is intuitively clear that the decomposable polynomials form a small minority among all polynomials (multivariate over a field). The goal in this work is to give a precise quantitative version of this intuition. Interestingly, we find a special case for bivariate polynomials where the intuition about the "most general decomposable polynomials" is incorrect.

We use the methods from von zur Gathen (2008c), where the corresponding task was solved for reducible, squareful, relatively irreducible, and singular bivariate polynomials; further references are given in that paper. Von zur Gathen, Viola & Ziegler (2009) extend those results to multivariate polynomials and give further information such as exact formulas and generating functions.

Our question has two facets: in the *geometric* view, we want to determine the dimension of the algebraic set of decomposable polynomials, say over an algebraically closed field. The *combinatorial* task is to approximate the number of decomposables over a finite field, together with a good relative error bound. The goal is to have a bound that is exponentially decreasing in the input size. The choices we make in our calculations are guided by the goal of such bounds in a form which is as simple and universal as possible.

As mentioned above, a special case occurs for bivariate polynomials. Usually, the largest number of decompositions results from maximizing the number of choices for the right component. But for some special degrees—the squares of primes and numbers of RSA type—most bivariate decompositions arise from having a large number of choices for the left component. At three or more variables, all is uniform.

Giesbrecht (1988) was the first to consider a variant of our counting problem. He showed that the decomposable univariate polynomials form an exponentially small fraction of all univariate polynomials. My interest, dating back to the supervision of this thesis, was rekindled by my study of similar counting problems (von zur Gathen 2008c), and during a visit to Pierre Dèbes' group at Lille, where I received a preliminary version of Bodin, Dèbes & Najib (2009b).

The companion paper von zur Gathen (2008a) deals with decomposable univariate polynomials.

2. Decompositions

We have a field F, a positive integer r, and the polynomial ring $R = F[x_1, \ldots, x_r]$. We assume a degree-respecting term order on R, so that in particular the *leading term* $\mathrm{lt}(f)$ of an $f \in R$ is defined and $\deg \mathrm{lt}(f) = \deg f$. Throughout this paper, deg denotes the total degree. If $f \neq 0$, the constant coefficient $\mathrm{lc}(f) \in F^\times = F \smallsetminus \{0\}$ of $\mathrm{lt}(f)$ is the *leading coefficient* of f. Then f is *monic* if $\mathrm{lc}(f) = 1$. We call f *original* if its graph contains the origin, that is, $f(0, \ldots, 0) = 0$.

The reader might think of the usual degree-lexicographic ordering, where terms of higher degree come before those of lower degree, and terms of the same degree are sorted lexicographically, with $x_1 > x_2 > \cdots > x_r$. For example,

$$f = -3x_1^2x_3 - 2x_2^3 + 4x_4x_5^2 + 5x_1^2 + 8x_1x_2 + 5x_6^2 - 7$$

is written in order, $\mathrm{lc}(f) = -3$ (provided that $-3 \neq 0$), and f is not original (if $-7 \neq 0$).

Definition 2.1. *For $g \in F[t]$ and $h \in R$,*

$$f = g \circ h = g(h) \in R$$

is their composition. *If $\deg g \geq 2$ and $\deg h \geq 1$, then (g, h) is a* decomposition *of f. A polynomial $f \in R$ is* decomposable *if there exist such g and h. Otherwise f is* indecomposable. *The decomposition (g, h) is* normal *if h is monic and original. It is* superlinear *if $\deg h \geq 2$.*

There are other notions of decompositions. The present one is called uni-multivariate in von zur Gathen *et al.* (2003). Another one is studied in Faugère & Perret (2008) for cryptanalytic purposes. In the context of univariate polynomials, only superlinear decompositions are traditionally considered.

REMARK 2.2. *Multiplication by a unit or addition of a constant does not change decomposability, since*

$$f = g \circ h \Longleftrightarrow af + b = (ag + b) \circ h$$

for all f, g, h as above and $a, b \in F$ with $a \neq 0$. In other words, the set of decomposable polynomials is invariant under this action of $F^\times \times F$ on R.

Furthermore, any decomposition (g, h) can be normalized by this action, by taking $a = \mathrm{lc}(h)^{-1} \in F^\times$, $b = -a \cdot h(0, \ldots, 0) \in F$, $g^* = g((t - b)a^{-1}) \in F[t]$, and $h^* = ah + b$. Then $g \circ h = g^* \circ h^*$ and (g^*, h^*) is normal.

The following result is shown for $r \geq 2$ in Bodin *et al.* (2009b). It is trivially valid for $r = 1$, where

$$f(x_1) = f(t) \circ x_1 \tag{2.3}$$

for any $f \in F[x_1]$.

FACT 2.4. *Any polynomial in R has at most one normal decomposition with indecomposable right component.*

When the characteristic does not divide the degree of f, then this also follows from the algorithmic approach in von zur Gathen (1990), and also holds for superlinear decompositions of univariate polynomials. If we also allowed trivial decompositions $f = g \circ h$ with $\deg g = 1$, then every polynomial would have exactly one normal decomposition with indecomposable right component.

We fix some notation for the remainder of this paper. For $r \geq 1$ and $n \geq 0$, we write

$$P_{r,n} = \{f \in F[x_1, \ldots, x_r] \colon \deg f \leq n\}$$

for the vector space of polynomials of degree at most n, of dimension

$$\dim P_{r,n} = b_{r,n} = \binom{r+n}{r}.$$

Furthermore, we consider the subsets

$$P^{=}_{r,n} = \{f \in P_{r,n} \colon \deg f = n\},$$
$$P^{0}_{r,n} = \{f \in P^{=}_{r,n} \colon f \text{ monic and original}\}.$$

Over an infinite field, the first of these is the Zariski-open subset $P_{r,n} \smallsetminus P_{r,n-1}$ of $P_{r,n}$ and irreducible, taking $P_{r,-1} = \{0\}$. The second one is obtained by further imposing one equation and working modulo multiplication by units, so that

$$\begin{aligned} \dim P^{=}_{r,n} &= b_{r,n}, \\ \dim P^{0}_{r,n} &= b_{r,n}-2, \end{aligned}$$

with $P^{0}_{r,0} = \varnothing$. For any divisor e of n, we have the normal composition map

$$\gamma_{r,n,e}\colon \begin{array}{ccc} P^{=}_{1,e} \times P^{0}_{r,n/e} & \longrightarrow & P^{=}_{r,n}, \\ (g,h) & \longmapsto & g \circ h, \end{array}$$

corresponding to Definition 2.1. (Here $P^{=}_{1,e}$ consists of polynomials in $F[t]$ rather than in $F[x_1]$.) The set $D_{r,n}$ of all decomposable polynomials in $P^{=}_{r,n}$ satisfies

$$D_{r,n} = \bigcup_{1<e|n} \operatorname{im} \gamma_{r,n,e}. \tag{2.5}$$

In particular, $D_{r,1} = \varnothing$ for all $r \geq 1$. Over an algebraically closed field, the dimension of $D_{r,n}$ is taken to be the maximal dimension of its irreducible components. We also call

$$I_{r,n} = P^{=}_{r,n} \smallsetminus D_{r,n}$$

the set of indecomposable polynomials. Thus $I_{r,1} = P^{=}_{r,1}$ for $r \geq 1$.

Remark 2.6. *By Remark 2.2, over an algebraically closed field, the codimension of $D_{r,n}$ in $P^{=}_{r,n}$ equals that of $D_{r,n} \cap P^{0}_{r,n}$ in $P^{0}_{r,n}$. The same holds for $I_{r,n}$, and over a finite field for the corresponding fractions.*

In order to have a nontrivial concept also in the univariate case, where (2.3) holds, we introduced in Definition 2.1 the notion of superlinear decompositions $f = g \circ h$ where $\deg h \geq 2$. The set of all these is

$$D^{\mathrm{sl}}_{r,n} = \bigcup_{\substack{e|n \\ 1<e<n}} \operatorname{im} \gamma_{r,n,e}. \tag{2.7}$$

In particular, $D^{\mathrm{sl}}_{r,n} = \varnothing$ if n is prime. We also let $I^{\mathrm{sl}}_{r,n} = P^{=}_{r,n} \smallsetminus D^{\mathrm{sl}}_{r,n}$. In the present paper, we investigate this notion only for two or more variables. The univariate case is treated in von zur Gathen (2008b).

3. Dimension of decomposables

In this section, we determine the dimension of the set of decomposable polynomials over an algebraically closed field. This forms the basis for the counting result in the next section.

Throughout the paper, ℓ denotes the smallest prime factor of $n \geq 2$. In the following, we have to single out the following special case:

$$r = 2, n/\ell \text{ is prime and } n/\ell \leq 2\ell - 5. \tag{3.1}$$

The smallest examples are $n = \ell^2$ with $\ell \geq 5$, $n = 11 \cdot 13$, and $n = 11 \cdot 17$. In particular, ℓ and n/ℓ are always at least 5.

Theorem 3.2. *Let F be an algebraically closed field, $r \geq 1$, $n \geq 2$, let ℓ be the smallest prime divisor of n, and*

$$m = \begin{cases} n & \text{if (3.1) holds or } r = 1, \\ \ell & \text{otherwise.} \end{cases} \tag{3.3}$$

Then the following hold.

(i) $D_{r,n}$ has dimension

$$\dim D_{r,n} = \binom{r + n/m}{r} + m - 1.$$

(ii) If $r \geq 2$, then $I_{r,n}$ is a dense open subset of $P^{=}_{r,n}$, of dimension $\binom{r+n}{r}$.

(iii) We assume that $r \geq 2$. Then $D^{\mathrm{sl}}_{r,n} = \varnothing$ if n is prime, and otherwise

$$\dim D^{\mathrm{sl}}_{r,n} = \binom{r + n/\ell}{r} + \ell - 1.$$

Proof. The claim (i) for $r = 1$ follows from (2.3), and we assume $r \geq 2$ in the remainder of the proof.

(i) Each $\gamma_{r,n,e}$ is a polynomial map, and we have

$$\dim \operatorname{im} \gamma_{r,n,e} \leq \dim P^{=}_{1,e} + \dim P^{0}_{r,n/e} = b_{r,n/e} + e - 1. \tag{3.4}$$

We let $E = \{e \in \mathbb{N} \colon 1 < e \mid n\}$ be the index set in (2.5). When n is prime, then $e = n = \ell$ is the only element of E, and the upper bound $\dim D_{r,n} \leq r + n$

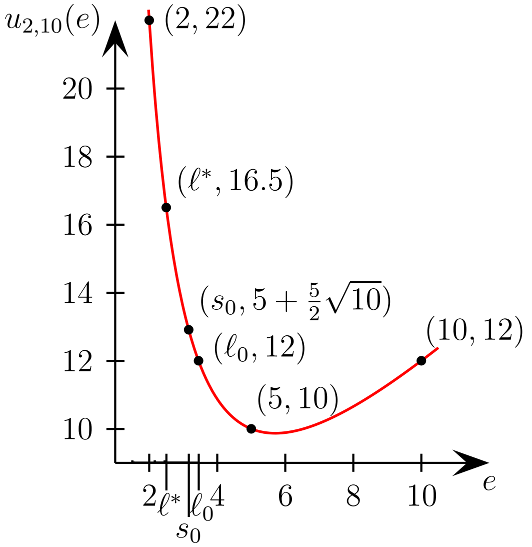

Figure 3.1: An example of $u_{r,n}$, for $r = 2$ and $n = 10$, with $\ell = 2$, $\ell^* = \frac{5}{2}$, $s_0 = \sqrt{10} \approx 3.16$, and $\ell_0 = 1 + \sqrt{6} \approx 3.45$.

in (i) follows. We may now assume that n is composite. We consider the right hand side in (3.4) as the function

$$u_{r,n}(e) = b_{r,n/e} + e - 1 \tag{3.5}$$

of a real variable e on the interval $[1, n]$. See Figure 3.1 for an example. We claim that

$$u_{r,n}(m) = \max_{e \in E} u_{r,n}(e). \tag{3.6}$$

The upper bound in (i) follows from this. The second derivative

$$\frac{\partial^2 u_{r,n}}{\partial e^2}(e) = \frac{n}{e^3 \cdot r!} \sum_{1 \le i \le r} \Big(\frac{n}{e} \sum_{\substack{1 \le j \le r \\ j \ne i}} \prod_{\substack{1 \le k \le r \\ k \ne i,j}} (k + \frac{n}{e}) + 2 \prod_{\substack{1 \le j \le r \\ j \ne i}} (j + \frac{n}{e}) \Big)$$

is positive on $[1, n]$, so that $u_{r,n}$ is convex. In particular, $u_{r,n}$ takes its maximum on the interval $[\ell, n]$ at one of the two endpoints.

For (3.6), we start with the case $r \ge 3$ and claim that $u_{r,n}(\ell) \ge u_{r,n}(n)$. Setting $s_0 = \sqrt{n}$, we have

$$u_{r,n}(s_0) - u_{r,n}(n) = \binom{r + s_0}{r} + s_0 - 1 - (r + s_0^2).$$

Now we replace s_0 by a real variable s, and set

$$v_r(s) = \binom{r+s}{r} + s - 1 - (r + s^2).$$

Then

$$v_r(2) = (r^2 + r - 4)/2 > 0, \tag{3.7}$$

since $r \geq 2$. Furthermore, we have

$$\frac{\partial v_r}{\partial s}(s) = \frac{1}{r!} \sum_{1 \leq i \leq r} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} (j + s) + 1 - 2s.$$

Expanding the product, we find that the coefficient in the sum of the linear term in s equals

$$\sum_{1 \leq i \leq r} \sum_{\substack{1 \leq j \leq r \\ j \neq i}} \prod_{\substack{1 \leq k \leq r \\ k \neq i,j}} k = r! \sum_{\substack{1 \leq i,j \leq r \\ j \neq i}} \frac{1}{i \cdot j} \geq r! \cdot 2 \cdot (\frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 3} + \frac{1}{2 \cdot 3}) = 2 \cdot r!,$$

since $r \geq 3$. Thus

$$\frac{\partial v_r}{\partial s}(s) \geq 0,$$

and together with (3.7) this implies $v_r(s) > 0$ for all $s \geq 2$. Since n is composite, we have $2 \leq \ell \leq \sqrt{n} = s_0 < n$, and from the above we have

$$u_{r,n}(\ell) \geq u_{r,n}(s_0) \geq u_{r,n}(n).$$

Since $m = \ell$, this shows the claim (3.6) and the upper bound in (i).

For the case $r = 2$, we observe that

$$u_{2,n}(\ell) - u_{2,n}(n) = \frac{(n - \ell)(n + 4\ell - 2\ell^2)}{2\ell^2} \tag{3.8}$$

is nonnegative if and only if $\ell \leq \ell_0$, where $\ell_0 = 1 + \frac{1}{2}\sqrt{2n+4}$ is the positive root of the quadratic factor. Furthermore, we note that

$$u_{2,n}(n) > u_{2,n}(\ell) \Longleftrightarrow \ell > \ell_0 \Longleftrightarrow n/\ell < 2\ell - 4 \Longleftrightarrow n/\ell \leq 2\ell - 5, \tag{3.9}$$

$$\ell_0^2 = n/2 + \sqrt{2n+4} + 2 > n/2.$$

If the conditions in (3.9) hold, there is at most one other prime factor of n besides ℓ, so that n/ℓ is prime and (3.1) holds. (3.6) follows in this case, and also otherwise because of the equivalences in (3.9).

We have now shown one inequality in (i), namely that $\dim D_{r,n} \leq u_{r,n}(m)$. For (ii), we claim that $u_{r,n}(m) < u_{r,n}(1) = \dim P^{=}_{r,n}$. Since $1 < m \leq n$ and $u_{r,n}$ is convex, it is sufficient to show that

$$r + n = u_{r,n}(n) < u_{r,n}(1) = \binom{r+n}{r}.$$

The inequality is equivalent to

$$r! < (r + n - 1)^{\underline{r-1}},$$

where $a^{\underline{r}} = a \cdot (a-1) \cdots (a - r + 1)$ is the falling factorial (or Pochhammer symbol). This is valid for $n = 2$ since $2 < r + 1$, and the right hand side is monotonically increasing in n, so that the claim is proven.

It follows that $D_{r,n}$ is contained in a proper closed subset of $P^{=}_{r,n}$, and there is a dense open subset consisting of indecomposable polynomials, which is (ii). This fact also holds in each $P^{=}_{r,n/e}$, and in $P^{0}_{r,n/e}$ by Remark 2.6. From the uniqueness of normal decompositions with indecomposable right factor (Fact 2.4) we conclude that each fiber of the restriction of $\gamma_{r,n,e}$ to $P^{=}_{1,e} \times I^{0}_{r,n/e}$ consists of a single point. Thus equality holds in (3.4), and (i) is also proven.

(iii) For superlinear compositions, we have $D^{\mathrm{sl}}_{r,n} = \varnothing$ if n is prime, and now may assume n to be composite. The maximal value allowed for e in (2.7) is n/ℓ. Thus (iii) follows from (i) when $m < n$. For $r = 2$,

$$u_{2,n}(\ell) - u_{2,n}(n/\ell) = \frac{(n - \ell^2)(n + \ell^2 + \ell)}{2\ell^2} \tag{3.10}$$

is always nonnegative, so that

$$\dim D^{\mathrm{sl}}_{2,n} = \dim \operatorname{im} \gamma_{2,n,\ell} = u_{2,n}(\ell).$$

Together with the uniqueness of Fact 2.4, this proves (iii) also for $r = 2$. □

4. Counting decomposables over finite fields

The goal in this section is to approximate the number of multivariate decomposables over a finite field, with a good relative error bound.

Over a finite field $F = \mathbb{F}_q$ with q elements, we have

$$\begin{aligned} \#P^{=}_{r,n} &= q^{b_{r,n}} - q^{b_{r,n-1}} = q^{b_{r,n}}(1 - q^{-b_{r-1,n}}), \\ \#P^{0}_{r,n} &= \frac{\#P^{=}_{r,n}}{q \cdot (q-1)} = q^{b_{r,n}-2}\frac{1 - q^{-b_{r-1,n}}}{1 - q^{-1}}. \end{aligned}$$

The proof of the following estimate of $\#D_{r,n}$ involves several case distinctions which are reflected in the somewhat complicated statement of the theorem. A simplified version is presented in Corollary 4.22 below.

Theorem 4.1. *Let $F = \mathbb{F}_q$ be a finite field with q elements, $r \geq 2$, ℓ the smallest prime divisor of $n \geq 2$, and m as in (3.3). We set*

$$\begin{aligned} \alpha_{r,n} &= q^{\binom{r+n/m}{r}+m-1}(1 - q^{-\binom{r-1+n/m}{r-1}}), \\ c_{r,n,1} &= \ell - 3, \\ c_{r,n,2} &= \ell - 2, \\ c_{r,n,3} &= \binom{r+1}{2} - 2, \\ c_{r,n,4} &= \binom{r-1+n/\ell}{r-1} - 1, \end{aligned} \tag{4.2}$$

$$\beta_{r,n} = \begin{cases} 0 & \text{if } n \text{ is prime}, \\ \dfrac{2q^{-c_{r,n,1}}(1 - q^{-n/\ell-1})}{1 - q^{-2}} & \text{if (3.1) holds}, \\ 2q^{-c_{r,n,2}} & \text{if } r = 2 \text{ and } n/\ell = 2\ell - 3 \text{ is prime}, \\ q^{-c_{r,n,3}} & \text{if } n = 4, \\ \dfrac{2q^{-c_{r,n,4}}}{1 - q^{-1}} & \text{otherwise}. \end{cases} \tag{4.3}$$

Then the following hold.

(i)

$$|\#D_{r,n} - \alpha_{r,n}| \leq \alpha_{r,n} \cdot \beta_{r,n}.$$

(ii)

$$\#I_{r,n} \geq \#P^{=}_{r,n} - 2\alpha_{r,n}.$$

(iii) We set

$$\alpha^{\mathrm{sl}}_{r,n} = \begin{cases} 0 & \text{if } n \text{ is prime}, \\ q^{\binom{2+n/\ell}{2}+\ell-1}(1-q^{-n/\ell-1}) & \text{if (3.1) holds}, \\ \alpha_{r,n} & \text{otherwise}, \end{cases}$$

$$\beta^{\mathrm{sl}}_{r,n} = \begin{cases} q^{-(n+\ell^2+\ell)(n-\ell^2)/2\ell^2} & \text{if (3.1) holds and } n > \ell^2, \\ q^{-(n+\ell-2)/2} & \text{if (3.1) holds and } n = \ell^2, \\ \beta_{r,n} & \text{otherwise.} \end{cases}$$

Then

$$\left|\#D^{\mathrm{sl}}_{r,n} - \alpha^{\mathrm{sl}}_{r,n}\right| \le \alpha^{\mathrm{sl}}_{r,n} \cdot \beta^{\mathrm{sl}}_{r,n}. \tag{4.4}$$

(iv) $\#I^{\mathrm{sl}}_{r,n} \ge \#P^{=}_{r,n} - 2\alpha^{\mathrm{sl}}_{r,n}$.

Proof. The proof of (i) and (ii) proceeds in three stages: an upper bound on decomposables, a lower bound on indecomposables, and a lower bound on decomposables. Each stage depends on the previous one.

According to (4.3), we have to distinguish five cases:

i	condition for case i	m	$c_{r,n,i}$
0	n prime	n	
1	$r=2$, $n/\ell \le 2\ell-5$ prime	n	$\ell-3$
2	$r=2$, $n/\ell = 2\ell-3$ prime	ℓ	$\ell-2$
3	$n=4$	ℓ	$\binom{r+1}{2}-2$
4	otherwise	ℓ	$\binom{r-1+n/\ell}{r-1}-1$

In the first stage, for a divisor e of n, we have

$$\#\operatorname{im}\gamma_{r,n,e} \le \#P^{=}_{1,e} \cdot \#P^{0}_{r,n/e} = q^{b_{r,n/e}+e-1}(1-q^{-b_{r-1,n/e}}),$$

and thus with $u_{r,n}$ from (3.5)

$$\#D_{r,n} \le \sum_{1<e|n} \#\operatorname{im}\gamma_{r,n,e} \le \sum_{1<e|n} q^{u_{r,n}(e)}(1-q^{-b_{r-1,n/e}}). \tag{4.5}$$

We write u for $u_{r,n}$ and c_i for $c_{r,n,i}$, and recall $E = \{e \in \mathbb{N} \colon 1 < e \mid n\}$.

If n is prime, then $E = \{n\}$, $m = \ell = n$ (see (3.3)), and each right hand component h in a decomposition is linear, hence indecomposable. It follows from Fact 2.4 that $\gamma_{r,n,n}$ is injective, $D_{r,n} = \operatorname{im}\gamma_{r,n,n}$, and $\#D_{r,n} = \alpha_{r,n}$. All claims follow in this case.

In the first stage, we may use the following blanket assumptions and notations:

$$r \geq 2, a = n/\ell \geq \sqrt{n} \geq \ell \geq 2, a^2 \geq n \geq 2\ell \geq \ell + 2. \tag{4.6}$$

We first explain our general strategy for the upper bound

$$\#D_{r,n} \leq \alpha_{r,n}(1 + \beta_{r,n}) \tag{4.7}$$

in (i). From (3.6) we know that the maximal value of u occurs at $e = m$. By the convexity of u, each value is assumed at most twice, and we can majorize the sum in (4.5) by twice a geometric sum. However, this would provide an unsatisfactory error estimate, and we want to show that the difference between $u(m)$ and the other values $u(e)$ with $e \in E$ is sufficently large. We abbreviate

$$w = \frac{1 - q^{-b_{r-1,n/\ell}}}{1 - q^{-b_{r-1,n/m}}},$$

define δ, μ, and β in (4.8), and claim that for any c the following implication holds:

$$\left.\begin{array}{rcl} c \leq \delta & = & \min_{e \in E \smallsetminus \{m\}}(u(m) - u(e)) \\ \mu & = & \min\{\#E - 1, \frac{2}{1-q^{-1}}\} \\ \beta & = & \mu w q^{-c} \end{array}\right\} \Rightarrow \#D_{r,n} \leq \alpha_{r,n}(1 + \beta). \tag{4.8}$$

In our four cases, c will be instantiated by c_1, c_2, c_3, and c_4. We note that $\mu \leq 4$. In order to prove the claim, we note that

$$u(e) - u(m) \leq -c$$

for all $e \in E \smallsetminus \{m\}$. Since $b_{r-1,k}$ is monotonically increasing in k and $n/e \leq n/\ell$, we have

$$1 - q^{-b_{r-1,n/e}} \leq 1 - q^{-b_{r-1,n/\ell}}$$

for all $e \in E$. Using this estimate for all $e \neq m$ and the fact that the convex function u takes any of its values at most twice, we find that

$$\begin{aligned} q^{-u(m)} \sum_{e \in E} q^{u(e)}(1 - q^{-b_{r-1,n/e}}) &< (1 + 2w \sum_{i \leq -c} q^i) \cdot (1 - q^{-b_{r-1,n/m}}) \\ &= (1 + \frac{2wq^{-c}}{1 - q^{-1}}) \cdot (1 - q^{-b_{r-1,n/m}}). \end{aligned}$$

Also, since $E \setminus \{m\}$ has $\#E-1$ elements, we find

$$q^{-u(m)} \sum_{e \in E} q^{u(e)}(1-q^{-b_{r-1,n/e}}) \leq (1+(\#E-1)wq^{-c}) \cdot (1-q^{-b_{r-1,n/m}}).$$

Using (4.5) we conclude that

$$\#D_{r,n} \leq q^{u(m)}(1-q^{-b_{r-1,n/m}}) \cdot (1+\mu w q^{-c}) = \alpha_{r,n}(1+\beta), \tag{4.9}$$

as claimed. It then remains to see that $\beta \leq \beta_{r,n}$.

We now turn to our four cases. In case 1, (3.1) holds, $E = \{\ell, n/\ell, n\}$, $r=2$, $\ell \geq 5$, $m=n$, and

$$w = \frac{1-q^{-n/\ell-1}}{1-q^{-2}}.$$

Now (3.10) says that

$$u(\ell)-u(n/\ell) = \frac{(n-\ell^2)(n+\ell^2+\ell)}{2\ell^2} \geq 0,$$

so that $u(e) \leq u(\ell)$ for all $e \in E \setminus \{m\} = \{\ell, n/\ell\}$, and by (3.8)

$$\delta = u(n)-u(\ell) = \frac{1}{2}(\frac{n}{\ell}-1)(2\ell-4-\frac{n}{\ell}) > 0.$$

The two right hand factors are positive integers. If the second one equals 1, then

$$\delta = \frac{1}{2}(2\ell-5-1) = \ell-3 = c_1.$$

Otherwise, $\delta \geq n/\ell-1 \geq \ell-1 > \ell-3 = c_1$. Thus the assumptions in (4.8) hold with $c=c_1$, and since $\#E \leq 3$, we have $\mu \leq 2$ and $\beta \leq 2wq^{-c} = \beta_{r,n}$. This shows (4.7) in case 1.

In case 2, we have $E = \{\ell, 2\ell-3, n\}, m=\ell$, and

$$\begin{aligned} u(\ell)-u(n) &= \ell-2, \\ u(\ell)-u(2\ell-3) &= \frac{1}{2}(\ell-3)(3\ell-2). \end{aligned}$$

The minimum of these two values is $\ell-2$ when $\ell \geq 5$. Then $\delta = \ell-2 = c_2$, and furthermore $\mu = 2$ and $w=1$. This implies (4.7) in case 2, when $\ell \geq 5$. For $\ell = 3$, we have $n=9$, $E=\{3,9\}$, $u(3)=12$, $u(9)=11$, $\delta = 1 = \ell-2 = c_2$, $\mu=1$, and $w=1$. Thus $\beta = q^{-c_2} < \beta_{r,n}$, and (4.7) again holds.

In case 3, we have $E = \{2, 4\}$, $\ell = m = 2$, $w = \mu = 1$,

$$\delta = u(2) - u(4) = \binom{r+1}{2} - 2 = c_3 \geq 1,$$

and (4.7) holds.

In case 4, we have $m = \ell < n$, and introduce $\ell^* = n\ell/(n-\ell) \in \mathbb{Q}$. ($\ell^*$ is not an integer unless n is 4 or 6.) We first claim that

$$u(n) \leq u(\ell^*). \tag{4.10}$$

We start with the subcase $r \geq 3$ and have to show that

$$\binom{r+a-1}{r} + \frac{n}{a-1} - 1 = u(\ell^*) \geq u(n) = r + n. \tag{4.11}$$

We first treat the subcase $a \geq 5$. Then $a^3 \geq 3a^2 + 4a + 12$, so that the first inequality in

$$\begin{aligned} \frac{1}{a-1}\binom{r+a-2}{a-2} &= \frac{1}{r+a-1}\binom{r+a-1}{r} \\ &\geq 1 + \frac{a^2}{r+a-1} \geq 1 + \frac{n}{r+a-1} \end{aligned} \tag{4.12}$$

is valid for $r = 3$, and for all $r \geq 3$ since the left hand side is monotonically increasing and the right hand side decreasing in r. Using (4.6), this yields (4.11).

In the remaining subcase $r \geq 3$ and $a \leq 4$, we have $n \in \{4, 6, 8, 9\}$. Case 3 covers $n = 4$. The inequality between the outer terms in (4.12) holds for the following values of (r, n): $(4, 6)$, $(3, 8)$, and $(4, 9)$, and by monotonicity for these values of n and any larger r. One checks (4.11) for $(3, 6)$ and $(3, 9)$.

We next have the subcase $r = 2$ and $a \geq 3$. Then

$$\begin{aligned} u(n) - u(\ell^*) &= \frac{a-2}{2a-2} \cdot (2n - a^2 - 2a + 3), \\ u(n) > u(\ell^*) &\iff 2a\ell = 2n > a^2 + 2a - 3 \\ &\iff 2\ell > a + 2 - \frac{3}{a} \iff 2\ell \geq a + 2 \iff 2\ell - 2 \geq a. \end{aligned} \tag{4.13}$$

By assumption, (3.1) does not hold, and if (4.13) is positive, then $2\ell - 4 \leq a \leq 2\ell - 2$ follows. If a is even, then $\ell = 2$, and one finds that $n = 4$, which is case

3. So the only remaining possibility is $a = 2\ell - 3$. Since each prime divisor of a is at least ℓ, a is prime. But this is case 2, and therefore (4.10) holds.

For the remaining possibility $a = 2$, we find $\ell = 2$ and $n = 4$, which has been dealt with. We conclude that (4.10) always holds in case 4.

We have

$$\ell^2 + 2\ell < 2n$$

for all $n \neq 4$, since this follows from $n \geq \ell^2$ when $\ell \geq 3$, and also for $\ell = 2$. This implies that

$$\ell^* - \ell = \frac{\ell}{n/\ell - 1} < 2.$$

For any $e \in E \smallsetminus \{\ell\}$, we have $\ell < e \leq n$ and $n/e < n/\ell$. These values are both integers, so that

$$\frac{n}{e} \leq \frac{n}{\ell} - 1 = \frac{n}{\ell^*}.$$

Thus $\ell^* \leq e \leq n$ for all $e \in E \smallsetminus \{\ell\}$. By (4.10) and the convexity of u, the maximal value of $u(e)$ for these e is at most $\max\{u(\ell^*), u(n)\} = u(\ell^*)$. In (4.8) we have

$$\begin{aligned} \delta \geq u(\ell) - u(\ell^*) &= \binom{r + n/\ell}{r} - \binom{r - 1 + n/\ell}{r} + \ell - \ell^* \\ &= \binom{r - 1 + n/\ell}{r - 1} + \ell - \ell^* > c_4 + 1 - 2 = c_4 - 1. \end{aligned}$$

Since δ and c_4 are integers, we also have $\delta \geq c_4$. Furthermore, we have $w = 1$ and $\mu \leq 2(1 - q^{-1})^{-1}$, so that $\beta \leq \beta_{r,n}$. Then the assumptions in (4.8) hold with $c = c_4$, and (4.7) follows.

In the next stage, we derive the lower bound in (ii) on the number $\# I_{r,n}$ of indecomposable polynomials. The previous results yield

$$\# P^{=}_{r,n} - \# I_{r,n} = \# D_{r,n} \leq \alpha_{r,n}(1 + \beta_{r,n}).$$

The claim in (ii) is that the last expression is at most $2\alpha_{r,n}$, that is, $\beta_{r,n} \leq 1$. Again, we distinguish according to our four cases.

For case 1, we have $\ell \geq 5$ and $(1 - q^{-2})^{-1} \leq 4/3$, and thus $\beta_{r,n} < \frac{8}{3} q^{-\ell+3} \leq \frac{8}{3} \cdot 2^{-2} < 1$.

In case 2, we have $\ell \geq 3$ and

$$\beta_{r,n} = 2q^{-\ell+2} \leq q^{-\ell+3} \leq 1.$$

In case 3, we have $c_3 = \binom{r+1}{2} - 2 \geq 1 > 0$ and $\beta_{r,4} = q^{-c_3} < 1$.

In case 4, we have $\beta_{r,n} \leq 4q^{-c_4} \leq q^{2-c_4}$, so that it is sufficient to show that $c_4 \geq 2$. We have $r, a \geq 2$ and

$$c_4 + 1 = \binom{r-1+a}{r-1} \geq \binom{r+1}{r-1} = \frac{r \cdot (r+1)}{2} \geq 3.$$

This concludes the proof of (ii).

In the last stage, we estimate the number of decomposable polynomials from below. The idea is obvious: we take the largest type of decomposable polynomials, as identified above, and then use only indecomposable polynomials as right components, so that the uniqueness property of Fact 2.4 applies. We set

$$I^0_{r,n} = I_{r,n} \cap P^0_{r,n}.$$

By Remark 2.6 and (ii), we have

$$\begin{aligned}\#I^0_{r,n} &= \#I_{r,n} \cdot \frac{\#P^0_{r,n}}{\#P^=_{r,n}} \geq \frac{(\#P^=_{r,n} - 2\alpha_{r,n}) \cdot \#P^0_{r,n}}{\#P^=_{r,n}} \\ &= (1 - \frac{2\alpha_{r,n}}{\#P^=_{r,n}}) \frac{q^{b_{r,n}-2}(1 - q^{-b_{r-1,n}})}{1 - q^{-1}}.\end{aligned}$$

Thus

$$\begin{aligned}\#D_{r,n} &\geq \#\gamma_{r,n,m}(P^=_{1,m} \times I^0_{r,n/m}) = \#(P^=_{1,m} \times I^0_{r,n/m}) \\ &\geq q^{b_{r,n/m}+m-1}(1 - \frac{2\alpha_{r,n/m}}{\#P^=_{r,n/m}})(1 - q^{b_{r-1,n/m}}) = \alpha_{r,n} \cdot (1 - \frac{2\alpha_{r,n/m}}{\#P^=_{r,n/m}}).\end{aligned}$$

In the cases 2 and 3, n/m is prime, $\beta_{r,n/m} = 0$, and we could replace the factor 2 in the last expression by 1; however, we do not need this in the following. In order to prove the lower bound in (i), we proceed according to our four cases. In case 1, we have $r = 2$, (3.1) holds, $m = n$, and

$$\#D_{r,n} \geq \# \operatorname{im} \gamma_{r,n,n} = \#(P^=_{1,n} \times P^0_{r,1}) = \alpha_{r,n}. \tag{4.14}$$

For the remaining three cases, we have $m = \ell$ and claim that

$$\frac{2\alpha_{r,n/\ell}}{\#P^=_{r,n/\ell}} \leq \beta_{r,n}, \tag{4.15}$$

from which the lower bound follows:

$$\#D_{r,n} \geq \alpha_{r,n} \cdot (1 - \frac{2\alpha_{r,n/\ell}}{\#P^=_{r,n/\ell}}) \geq \alpha_{r,n} \cdot (1 - \beta_{r,n}).$$

We denote by m^* the quantity defined in (3.3) for the argument $a = n/\ell$ instead of n (and hence using the smallest prime divisor of n/ℓ instead of ℓ), and set $d = a/m^* = n/\ell m^*$. Thus m^* is either a or its smallest prime divisor, $a = m^*d \geq 2d \geq 2$, and

$$\frac{2\alpha_{r,a}}{\#P^{=}_{r,a}} = \frac{2q^{-c^*}(1-q^{-b_{r-1,d}})}{1-q^{-b_{r-1,a}}} \leq 2q^{-c^*}, \tag{4.16}$$

with

$$c^* = \binom{r+a}{r} - \binom{r+d}{r} - m^* + 1.$$

It is therefore sufficient for (4.15) to show

$$2q^{-c^*} \leq \beta_{r,n}. \tag{4.17}$$

In case 2, $m^* = a = n/\ell = 2\ell - 3$ is prime, and

$$c^* = (2\ell-1)(\ell-2) > \ell - 2,$$
$$2q^{-c^*} < 2q^{-(\ell-2)} = \beta_{2,n},$$

and (4.17) is satisfied.

In case 3, we have $n = 4$, $\ell = 2$, $a = m^* = 2$, $d = 1$, $c^* = \binom{r+1}{2} - 1$, and thus

$$2q^{-c^*} \leq q \cdot q^{-\binom{r+1}{2}+1} = \beta_{r,4}.$$

In case 4, we have

$$\beta_{r,n} = \frac{2q^{-c_4}}{1-q^{-1}} > 2q^{-c_4},$$

and it is sufficient for (4.17) to show that

$$c^* \geq c_4, \tag{4.18}$$

which in turn amounts to showing that

$$\binom{r-1+a}{r} = \binom{r+a}{r} - \binom{r-1+a}{r-1} \geq \binom{r+d}{r} + m^* - 2, \tag{4.19}$$

using Pascal's identity. We prove this by induction on $r \geq 2$. For $r = 2$, we use $a = m^*d \geq m^* \geq 2$. Thus

$$a^2 + a - (\frac{a}{m^*})^2 - 3\frac{a}{m^*} = \frac{a}{(m^*)^2}\big(a((m^*)^2-1) + (m^*)^2 - 3m^*\big) \geq 2m^* - 2,$$

since the inequality holds for $a = m^*$ and the middle term is monotonically increasing in a for $m^* \geq 2$. It follows that

$$a^2 + a \geq (\frac{a}{m^*})^2 + 3\frac{a}{m^*} + 2m^* - 2,$$

which implies (4.19) for $r = 2$.

For the induction step, we have $a - 1 \geq a/2 \geq a/m^* = d$, and

$$\binom{r+a-1}{r} - \binom{r+d}{r} \geq \binom{r-1+a-1}{r-1} - \binom{r-1+d}{r-1} \geq m^* - 2,$$

again by Pascal.

This finishes the proof of (i), and it remains to prove (iii) and (iv). We may assume n to be composite. Since $D^{\mathrm{sl}}_{r,n} \subseteq D_{r,n} = D^{\mathrm{sl}}_{r,n} \cup \operatorname{im} \gamma_{r,n,n}$, the upper bound on $\#D_{r,n}$ in (i) also holds for $\#D^{\mathrm{sl}}_{r,n}$, and the lower bound does unless $m = n$. Thus (iii) and (iv) follow unless (3.1) holds, which we now assume.

Since $n/\ell \geq \ell$, we have $1 - q^{-n/\ell-1} \geq 1 - q^{-\ell-1}$. Using (3.10), we find

$$\begin{aligned}
\#D^{\mathrm{sl}}_{2,n} &\leq \#(P^{=}_{1,\ell} \times P^{0}_{2,n/\ell}) + \#(P^{=}_{1,n/\ell} \times P^{0}_{2,\ell}) \\
&= \alpha^{\mathrm{sl}}_{2,n}(1 + q^{-(n+\ell^2+\ell)(n-\ell^2)/2\ell^2}\frac{1-q^{-\ell-1}}{1-q^{-n/\ell-1}}) \leq \alpha^{\mathrm{sl}}_{2,n}(1+\beta^{\mathrm{sl}}_{2,n}), \\
\#D^{\mathrm{sl}}_{2,n} &\geq \#(P^{=}_{1,\ell} \times I^{0}_{2,n/\ell}) \\
&\geq \#P^{=}_{1,\ell} \cdot (\#P^{=}_{2,n/\ell} - 2\alpha_{2,n/\ell}) \cdot \frac{\#P^{0}_{2,n/\ell}}{\#P^{=}_{2,n/\ell}} \\
&= \alpha^{\mathrm{sl}}_{2,n}(1 - 2q^{-(n+2\ell)(n-\ell)/2\ell^2}\frac{1-q^{-2}}{1-q^{-n/\ell-1}}) \\
&\geq \alpha^{\mathrm{sl}}_{2,n}(1 - q^{-(n+2\ell)(n-\ell)/2\ell^2+1}) \\
&> \alpha^{\mathrm{sl}}_{2,n}(1-\beta^{\mathrm{sl}}_{2,n}).
\end{aligned}$$

If $n = \ell^2$, then $D^{\mathrm{sl}}_{2,n} = \operatorname{im} \gamma_{2,n,\ell}$ and

$$\begin{aligned}
\#D^{\mathrm{sl}}_{2,n} &\leq \#(P^{=}_{1,\ell} \times P^{0}_{2,\ell}) = \alpha^{\mathrm{sl}}_{2,n}, \\
\#D^{\mathrm{sl}}_{2,n} &\geq \#(P^{=}_{1,\ell} \times I^{0}_{2,\ell}) \geq \alpha^{\mathrm{sl}}_{2,n}(1 - \beta^{\mathrm{sl}}_{2,n}\frac{1-q^{-2}}{1-q^{-\ell-1}}) \geq \alpha^{\mathrm{sl}}_{2,n}(1-\beta^{\mathrm{sl}}_{2,n}). \qquad \square
\end{aligned}$$

Remark 4.20. *In the simple case where n has exactly two prime factors and $r \geq 2$, it is easy to determine $\#D_{r,n}$ exactly. For $n = \ell^2$,*

$$D_{r,n} = \gamma_{r,n,\ell}(P^{=}_{1,\ell} \times I^0_{r,\ell}) \cup \gamma_{r,n,n}(P^{=}_{1,n} \times I^0_{r,1})$$

is a disjoint union. We have

$$\#D_{r,n} = \begin{cases} \alpha_n + q^{(n+5\ell)/2}(1 - q^{-\ell-1}) - q^{2\ell+1}(1 - q^{-r}) & \text{if (3.1) holds,} \\ \alpha_n + q^{n+r}(1 - q^{-r})(1 - q^{2\ell-n-1}) & \text{otherwise.} \end{cases}$$

We set

$$\beta'_{r,n} = \begin{cases} q^{(-n+5\ell-4)/2} \dfrac{1 - q^{-\ell-1}}{1 - q^{-2}} - q^{-n+2\ell-1} & \text{if (3.1) holds,} \\ q^{n+r+1-\binom{r+n/\ell}{r}-\ell} \dfrac{(1 - q^{-r})(1 - q^{2\ell-n-1})}{1 - q^{-\binom{r-1+n/\ell}{r-1}}} & \text{otherwise.} \end{cases}$$

Then

$$\#D_{r,n} = \alpha_{r,n}(1 + \beta'_{r,n}).$$

This value is exact, in contrast to the estimates of Theorem 4.1, and $\beta'_{r,n}$ is often much smaller than $\beta_{r,n}$. The drawback is that the values are more complicated, and an attempt to generalize this approach to more than two prime factors of n does not seem to lead to manageable results.

If $n > \ell^2$ and n/ℓ is prime, then one finds similarly that

$$\begin{aligned} \#D_{r,n} &= q^{b_{r,n/\ell}+\ell-1}(1 - q^{-b_{r-1,n/\ell}}) + q^{b_{r,\ell}+n/\ell-1}(1 - q^{b_{r-1,\ell}}) \\ &\quad + q^{n+r}(1 - q^{-r})(1 - 2q^{\ell+n/\ell-n-1}). \end{aligned}$$

Here it is not even transparent which of the summands is the dominating one. However, using the case distinction of (3.1), one again obtains a quantity $\beta'_{r,n}$, so that $\#D_{r,n} = \alpha_{r,n}(1+\beta'_{r,n})$. The previous remarks apply to this solution as well.

Bodin *et al.* (2009b) obtain an equivalent result, in a different language. They also show that $\#I_{r,n}/\#P^{=}_{r,n} \to 1$ as $n \to \infty$ (see Theorem 4.1(ii)), and some results similar to those of Theorem 4.1(i) when either $r = 2$ or n has at most two prime factors. Their methods do not lead to a unified formula as in Theorem 4.1(i), and the error bounds are weaker than the present ones by factors of $O(n)$ or $O(q)$.

If $u_{2,n}(e) = u_{2,n}(e')$ never happened for distinct divisors e, $e' \geq 2$ of n, we could save a factor of 2 in $\beta_{2,n}$. However, if we take two arbitrary positive integers $k \geq 2$ and m, set $e = 2km^2 + 2m^2 + 3m$, $e' = ke$, and $n = 2mke$, then $e < e'$ and $u_{2,n}(e) = u_{2,n}(e')$. The smallest such choice gives $n = 36$, $e = 9$, $e' = 18$.

We can unify cases 2 and 4 in (4.3), and the other cases fit in trivially. We set

$$\begin{aligned} c_{r,n,5} &= \frac{1}{2}\binom{r-1+n/\ell}{r-1} - 1, \\ \beta^*_{r,n} &= \frac{2q^{-c_{r,n,5}}}{1-q^{-1}}. \end{aligned} \tag{4.21}$$

Corollary 4.22. *Let $D_{r,n}$ be the set of decomposable polynomials of degree $n \geq 2$ in $r \geq 2$ variables over $\mathbb{F}_q$, and $\alpha_{r,n}$ and $\beta^*_{r,n}$ as in (4.2) and (4.21), respectively. Then*

$$|\#D_{r,n} - \alpha_{r,n}| \leq \alpha_{r,n} \cdot \beta^*_{r,n}.$$

Proof. It is sufficient to show that $\beta_{r,n} \leq \beta^*_{r,n}$ in all cases. This is an easy calculation. □

How close is our relative error estimate $\beta_{r,n}$ to being exponentially decaying in the input size? In the "general" case 4 of (4.3), $\beta_{r,n}$ is about q^{-c_4} with c_4 approximately $b_{r-1,n/\ell} = \binom{r-1+n/\ell}{r-1}$. (4.21) and Corollary 4.22 relate also the special cases to this.

The (usual) dense representation of a polynomial in r variables and of degree at most n requires $b_{r,n} = \binom{r+n}{r}$ monomials, each of them equipped with a coefficient from $\mathbb{F}_q$, using about $\log_2 q$ bits. Thus the total input size is about $\log_2 q \cdot b_{r,n}$ bits. Now $\log_2 q \cdot b_{r,n/\ell}$ differs from $\log_2 \beta_{r,n}$ by a factor of $1 + \frac{n}{r\ell}$. Furthermore, n and n/ℓ are polynomially related, since $n > n/\ell \geq \sqrt{n}$. Up to these polynomial differences (in the exponent), $\beta_{r,n}$ is exponentially decaying in the input size. Furthermore $\beta_{r,n}$ is exponentially decaying in any of the parameters r, n and $\log_2 q$, when the other two are fixed.

We compare our results to those of von zur Gathen (2008c) on the number $\#R_n$ of reducible and $\#E_n$ of relatively irreducible (irreducible and not absolutely irreducible) bivariate polynomials. Ignoring small factors and special cases like (3.1), we have for composite n

$$\begin{aligned}\#R_n &\approx q^{\binom{n+2}{2}-n+1}\\ \#E_n &\approx q^{\binom{n+2}{2}-\frac{n^2(\ell-1)}{2\ell}}\\ \#D_{2,n} &\approx q^{\binom{n/\ell+2}{2}+\ell-1}.\end{aligned}$$

The first exponent is always greater than the third one, and for the second and third ones we have

$$\binom{n+2}{2}-\frac{n^2(\ell-1)}{2\ell}-\binom{n/\ell+2}{2}-\ell+1=\frac{(\ell-1)(n^2+3n\ell-2\ell^2)}{2\ell^2}>0.$$

In other words, there are many more reducible or relatively irreducible bivariate polynomials than decomposable ones, as one would expect.

5. Acknowledgements

I appreciate the interesting discussions with Arnaud Bodin, Pierre Dèbes, and Salah Najib about the topic, and in particular the challenges that the preliminary version of Bodin *et al.* (2009b) posed.

A first version of this paper is in von zur Gathen (2008a). The work was supported by the B-IT Foundation and the Land Nordrhein-Westfalen.

References

Arnaud Bodin, Pierre Dèbes & Salah Najib (2009b). Indecomposable polynomials and their spectrum. *To appear in Acta Arithmetica.*

Jean-Charles Faugère & Ludovic Perret (2008). High Order Derivatives and Decomposition of Multivariate Polynomials. In *Extended Abstracts of the Second Workshop on Mathematical Cryptology WmC 08*, Álvar Ibeas & Jaime Gutiérrez, editors, 90–93. URL http://grupos.unican.es/amac/wmc-2008/.

Joachim von zur Gathen (1990). Functional Decomposition of Polynomials: the Tame Case. *Journal of Symbolic Computation* **9**, 281–299.

Joachim von zur Gathen (2008a). Counting decomposable multivariate polynomials. *Preprint,* 21 pages. URL http://arxiv.org/abs/0811.4726.

Joachim von zur Gathen (2008b). Counting decomposable univariate polynomials. *Preprint,* 67 pages. URL http://arxiv.org/abs/0901.0054.

JOACHIM VON ZUR GATHEN (2008c). Counting reducible and singular bivariate polynomials. *Finite Fields and Their Applications* **14**(4), 944–978. URL http://dx.doi.org/10.1016/j.ffa.2008.05.005. Extended abstract in *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation ISSAC2007,* Waterloo, Ontario, Canada (2007), 369-376.

JOACHIM VON ZUR GATHEN, JAIME GUTIERREZ & ROSARIO RUBIO (2003). Multivariate polynomial decomposition. *Applicable Algebra in Engineering, Communication and Computing* **14**, 11–31. URL http://dx.doi.org/10.1007/s00200-003-0122-8. Extended abstract in *Proceedings of the Second Workshop on Computer Algebra in Scientific Computing, CASC '99,* München, Germany (1999), 463-478.

JOACHIM VON ZUR GATHEN, ALFREDO VIOLA & KONSTANTIN ZIEGLER (2009). Exact counting of reducible multivariate polynomials. *In preparation.*

MARK WILLIAM GIESBRECHT (1988). Complexity Results on the Functional Decomposition of Polynomials. Technical Report 209/88, University of Toronto, Department of Computer Science, Toronto, Ontario, Canada.

JOACHIM VON ZUR GATHEN
B-IT
Universität Bonn
D-53113 Bonn
gathen@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/